Compatible systems of symplectic Galois representations and the inverse Galois problem II. Transvections and huge image.

Sara Arias-de-Reyna*, Luis Dieulefait†, Gabor Wiese‡

1st March 2013

Abstract

This article is the second part of a series of three articles about compatible systems of symplectic Galois representations and applications to the inverse Galois problem.

This part is concerned with symplectic Galois representations having a huge residual image, by which we mean that a symplectic group of full dimension over the prime field is contained up to conjugation. We prove a classification result on those subgroups of a general symplectic group over a finite field that contain a nontrivial transvection. Translating this group theoretic result into the language of symplectic representations whose image contains a nontrivial transvection, these fall into three very simply describable classes: the reducible ones, the induced ones and those with huge image. Using the idea of an (n, p)-group of Khare, Larsen and Savin we give simple conditions under which a symplectic Galois representation with coefficients in a finite field has a huge image. Finally, we combine this classification result with the main result of the first part to obtain a strenghtened application to the inverse Galois problem.

MSC (2010): 11F80 (Galois representations); 20G14 (Linear algebraic groups over finite fields), 12F12 (Inverse Galois theory).

1 Introduction

This article is the second of a series of three about compatible systems of symplectic Galois representations and applications to the inverse Galois problem.

This part is concerned with symplectic Galois representations having a *huge image*: For a prime ℓ, a finite subgroup $G \subseteq \mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$ is called *huge* if it contains a conjugate (in $\mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$) of $\mathrm{Sp}_n(\mathbb{F}_\ell)$. By Corollary 1.3 below this notion is the same as the one introduced in Part I ([AdDW12]).

*Université du Luxembourg, Faculté des Sciences, de la Technologie et de la Communication, 6, rue Richard Coudenhove-Kalergi, L-1359 Luxembourg, Luxembourg, sara.ariasdereyna@uni.lu

†Departament d'Àlgebra i Geometria, Facultat de Matemàtiques, Universitat de Barcelona, Gran Via de les Corts Catalanes, 585, 08007 Barcelona, Spain, ldieulefait@ub.edu

‡Université du Luxembourg, Faculté des Sciences, de la Technologie et de la Communication, 6, rue Richard Coudenhove-Kalergi, L-1359 Luxembourg, Luxembourg, gabor.wiese@uni.lu

Whereas the classification of the finite subgroups of $\mathrm{Sp}_n(\overline{\mathbb{F}}_\ell)$ appears very complicated to us, it turns out that the finite subgroups containing a nontrivial transvection can be very cleanly classified into three classes, one of which is that of huge subgroups. This is the main group theoretic result of this article (see Theorem 1.1 below). Translating this group theoretic result into the language of symplectic representations whose image contains a nontrivial transvection, these also fall into three very simply describable classes: the reducible ones, the induced ones and those with huge image (see Corollary 1.2).

Using the idea of an (n, p)-group of [KLS08], some number theory allows us to give very simple conditions under which a symplectic Galois representation with coefficients in $\overline{\mathbb{F}}_\ell$ has huge image (see Theorem 1.4 below).

This second part is independent of the first, except for Corollary 1.5, which combines the main results of Part I, and Part II. In the third part of this series of articles, a compatible system satisfying the assumptions of Corollary 1.5 will be constructed. At the moment, the third part is in preparation.

Statement of the results

In order to fix terminology, we recall some standard definitions. Let K be a field. An n-dimensional K-vector space V equipped with a symplectic form (i.e. nonsingular and alternating), denoted by $\langle v, w\rangle = v \bullet w$ for $v, w \in V$, is called a symplectic K-space. A K-subspace $W \subseteq V$ is called a *symplectic K-subspace* if the restriction of $\langle v, w\rangle$ to $W \times W$ is nonsingular (hence, symplectic).

The *general symplectic group* $\mathrm{GSp}(V, \langle\cdot,\cdot\rangle) =: \mathrm{GSp}(V)$ consists of those $A \in \mathrm{GL}(V)$ such that there is $\alpha \in K^\times$, the *multiplier* of A, such that we have $(Av)\bullet(Aw) = \alpha(v\bullet w)$ for all $v, w \in V$. The *symplectic group* $\mathrm{Sp}(V, \langle\cdot,\cdot\rangle) =: \mathrm{Sp}(V)$ is the subgroup of $\mathrm{GSp}(V)$ of elements with multiplier 1.

An element $\tau \in \mathrm{GL}(V)$ is a *transvection* if $\tau - \mathrm{id}_V$ has rank 1, i.e. if τ fixes a hyperplane pointwisely, and there is a line U such that $\tau(v) - v \in U$ for all $v \in V$. The fixed hyperplane is called the *axis* of τ and the line U is the *centre* (or the *direction*). We will consider the identity as a "trivial transvection". Any transvection has determinant 1. A *symplectic transvection* is a transvection in $\mathrm{Sp}(V)$. Any symplectic transvection has the form

$$T_v[\lambda] \in \mathrm{Sp}(V) : u \mapsto u + \lambda\langle u, v\rangle v$$

with *direction vector* $v \in V$ and *parameter* $\lambda \in K$ (see e.g. [Art57], pp. 137–138).

Our classification result on subgroups of general symplectic groups containing a nontrivial transvection is the following.

Theorem 1.1. *Let K be a finite field of characteristic at least 5 and V a symplectic K-vector space of dimension n. Then any subgroup G of $\mathrm{GSp}(V)$ which contains a nontrivial symplectic transvection satisfies one of the following assertions:*

1. *There is a proper K-subspace $S \subset V$ such that $G(S) = S$.*

2. *There are nonsingular symplectic K-subspaces $S_i \subset V$ with $i = 1, \ldots, h$ of dimension m for some $m < n$ such that $V = \bigoplus_{i=1}^{h} S_i$ and for all $g \in G$ there is a permutation $\sigma_g \in \mathrm{Sym}_h$ (the symmetric group on $\{1, \ldots, h\}$) with $g(S_i) = S_{\sigma_g(i)}$. Moreover, the action of G on the set $\{S_1, \ldots, S_h\}$ thus defined is transitive.*

3. *There is a subfield L of K such that the subgroup generated by the symplectic transvections of G is conjugated (in $\mathrm{GSp}(V)$) to $\mathrm{Sp}_n(L)$.*

The main purpose Section 2 is to prove this theorem. For our application to Galois representations we provide the following representation theoretic reformulation of Theorem 1.1.

Corollary 1.2. *Let ℓ be a prime at least 5, let Γ be a compact topological group and*

$$\rho : \Gamma \to \mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$$

a continuous representation (for the discrete topology on $\overline{\mathbb{F}}_\ell$). Assume that the image of ρ contains a nontrivial transvection. Then one of the following assertions holds:

1. *ρ is reducible.*

2. *There is a closed subgroup $\Gamma' \subsetneq \Gamma$ of finite index $h \mid n$ and a representation $\rho' : \Gamma' \to \mathrm{GSp}_{n/h}(\overline{\mathbb{F}}_\ell)$ such that $\rho \cong \mathrm{Ind}_{\Gamma'}^{\Gamma}(\rho')$.*

3. *There is a subfield L of K such that the subgroup generated by the symplectic transvections in the image of ρ is conjugated (in $\mathrm{GSp}(V)$) to $\mathrm{Sp}_n(L)$; in particular, the image is huge.*

The following corollary shows that the definition of a huge subgroup of $\mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$, which we gave in Part I [AdDW12], coincides with the simpler definition stated above.

Corollary 1.3. *Let K be a finite field of characteristic $\ell \geq 5$, V a symplectic K-vector space of dimension n, and G a subgroup of $\mathrm{GSp}(V)$ which contains a symplectic transvection. Then the following are equivalent:*

(i) *G is huge.*

(ii) *G contains a subgroup which is conjugate (in $\mathrm{GSp}(V)$) to $\mathrm{Sp}_n(\mathbb{F}_\ell)$.*

(iii) *There is a subfield L of K such that the subgroup generated by the symplectic transvections of G is conjugated (in $\mathrm{GSp}(V)$) to $\mathrm{Sp}_n(L)$.*

Combining our group theoretic results with (n, p)-groups, introduced by [KLS08], some number theory allows us to prove the following theorem:

Theorem 1.4. *Let n be an even number, $k \in \mathbb{N}$ and $\ell > kn! + 1$ a prime number. Let $N \in \mathbb{N}$ be an integer, not divisible by ℓ, say $N = N_1 \cdot N_2$ with $\gcd(N_1, N_2) = 1$. Let L_0 be the compositum of all number fields of degree $\leq n/2$, which are ramified at most at the primes dividing N_2 (which is a*

number field). Let $q \neq \ell$ be a prime which is completely split in L_0, and let $p \neq \ell$ be a prime dividing $q^n - 1$ but not dividing $q^{\frac{n}{2}} - 1$, and $p \equiv 1 \pmod{n}$. Let $\chi_q : G_{\mathbb{Q}_{q^n}} \to \overline{\mathbb{Q}}_\ell^\times$ be a character satisfying the assumptions of Lemma 3.1, and $\overline{\chi}_q$ the composition of χ_q with the reduction map $\overline{\mathbb{Z}}_\ell \to \overline{\mathbb{F}}_\ell$.

Let

$$\rho : G_{\mathbb{Q}} \to \mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$$

be a Galois representation, regular of inertial weights at most k, ramified only at the primes dividing $Nq\ell$ such that (1) $\mathrm{Res}_{G_{\mathbb{Q}_q}}^{G_{\mathbb{Q}}}(\rho) = \mathrm{Ind}_{G_{\mathbb{Q}_{q^n}}}^{G_{\mathbb{Q}_q}}(\overline{\chi}_q)$, (2) the image of ρ contains a nontrivial transvection and (3) for all primes ℓ_1 dividing N_1, the image by ρ of I_{ℓ_1}, the inertia group at ℓ_1, has order prime to $n!$.

Then the image of ρ is a huge subgroup of $\mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$.

Combining Theorem 1.4 with the results of Part I of this series ([AdDW12]) yields the following corollary.

Corollary 1.5. *Let $n, N \in \mathbb{N}$ be integers with n even and $N = N_1 \cdot N_2$ with $\gcd(N_1, N_2) = 1$. Let L_0 be the compositum of all number fields of degree $\leq n/2$, which are ramified at most at the primes dividing N_2 (which is a number field). Let q be a prime which is completely split in L_0, and let p be a prime dividing $q^n - 1$ but not dividing $q^{\frac{n}{2}} - 1$, and $p \equiv 1 \pmod{n}$. Let $\chi_q : G_{\mathbb{Q}_{q^n}} \to \overline{\mathbb{Z}}^\times$ be a character such that its composite with $\overline{\mathbb{Z}}^\times \hookrightarrow \overline{\mathbb{Q}}_\ell^\times$ satisfies the assumptions of Lemma 3.1 for all primes $\ell \nmid pq$.*

Let $\rho_\bullet = (\rho_\lambda)_\lambda$(where λ runs through the finite places of a number field L) be an n-dimensional a. e. absolutely irreducible a.e. symplectic compatible system, as defined in Part I ([AdDW12]), for the base field $\mathbb{Q}$, which satisfies the following assumptions:

- *For all places λ the representation ρ_λ is unramified outside $Nq\ell$, where ℓ is the rational prime below λ.*
- *There is a positive integer k such that, for all but possibly finitely many places λ of L, the reduction mod λ of ρ_λ is regular in the sense of Definition 3.2, with inertial weights at most k.*
- *The multiplier of $\rho_\bullet$ is a finite order character times a power of the cyclotomic character.*
- *For all but possibly finitely many places λ the residual representation $\overline{\rho}_\lambda$ contains a nontrivial transvection in its image.*
- *For all places λ not above q one has $\mathrm{Res}_{G_{\mathbb{Q}_q}}^{G_{\mathbb{Q}}}(\rho_\lambda) = \mathrm{Ind}_{G_{\mathbb{Q}_{q^n}}}^{G_{\mathbb{Q}_q}}(\chi_q)$, where χ_q is embedded into $\overline{\mathbb{Q}}_\ell$ via λ.*
- *For all primes ℓ_1 dividing N_1 and for all but possibly finitely many places λ, the group $\overline{\rho}_\lambda(I_{\ell_1})$ has order prime to $n!$ (where I_{ℓ_1} denotes the inertia group at ℓ_1).*

Then for any $d \mid \frac{p-1}{n}$ there exists a set of places $\mathcal{L}_d$ of L of positive density such that for each $\lambda \in \mathcal{L}_d$ the image of $\overline{\rho}_\lambda^{\mathrm{proj}}$ is $\mathrm{PGSp}_n(\mathbb{F}_{\ell^d})$ or $\mathrm{PSp}_n(\mathbb{F}_{\ell^d})$, where ℓ is the rational prime below λ.

The proofs of Theorem 1.4 and Corollary 1.5 are given in Section 3.

Acknowledgements

S. A.-d.-R. worked on this article as a fellow of the Alexander-von-Humboldt foundation. She thanks the Université du Luxembourg for its hospitality during a long term visit in 2011. She was also partially supported by MEC grant MTM2009-07024. G. W. was partially supported by the Sonderforschungsbereich TRR 45, the DFG priority program 1489 and by the Université du Luxembourg. S. A.-d.-R. and G. W. thank the Centre de Recerca Matemàtica for its support and hospitality during a long term visit in 2010.

2 Symplectic representations containing a transvection

In this section our group theoretic results will be proved. This part was inspired by the work of Mitchell on the classification of subgroups of classical groups. In an attempt to generalise Theorem 1 of [Mit14] to arbitrary dimension, one of us (S. A.-d.-R.) came up with a precise strategy for Theorem 1.1. Several ideas and some notation are borrowed from [LZ82].

2.1 Symplectic transvections in subgroups

Recall that the full symplectic group is generated by all its transvections. The main idea in this part is to identify the subgroups of the general symplectic group containing a transvection by the centres of the transvections in the subgroup.

Let K be a finite field of characteristic ℓ and V a symplectic K-vector space of dimension n. Let G be a subgroup of $\mathrm{GSp}(V)$. A main difficulty in this part stems from the fact that K need not be a prime field, whence the set of direction vectors of the transvections contained in G need not be a K-vector space. Suppose, for example, that we want to deal with the subgroup $G = \mathrm{Sp}_n(L)$ of $\mathrm{Sp}_n(K)$ for L a subfield of K. Then the directions of the transvections of G form the L-vector space L^n contained in K^n. It is this what we have in mind when we introduce the term (L, G)-rational subspace below. In order to do so, we set up some more notation.

Write $\mathcal{L}(G)$ for the set of $0 \neq v \in V$ such that $T_v[\lambda] \in G$ for some $\lambda \in K$. More naturally, this set should be considered as a subset of $\mathbb{P}(V)$, the projective space consisting of the lines in V. We call it the *set of centres (or directions) of the symplectic transvections in* G. For a given nonzero vector $v \in V$, define the *parameter group of direction* v *in* G as

$$\mathcal{P}_v(G) := \{\lambda \in K \mid T_v[\lambda] \in G\}.$$

The fact that $T_v(\mu) \circ T_v(\lambda) = T_v(\mu + \lambda)$ shows that $\mathcal{P}_v(G)$ is a subgroup of the additive group of K. If K is a finite field of characteristic ℓ, then $\mathcal{P}_v(G)$ is a finite direct product of copies of $\mathbb{Z}/\ell\mathbb{Z}$. Denote the number of factors by $\mathrm{rk}_v(G)$. Because of $\mathcal{P}_{\lambda v}(G) = \frac{1}{\lambda^2}\mathcal{P}_v(G)$ for $\lambda \in K^\times$, it only depends on the centre $U := \langle v \rangle_K \in \mathcal{L}(G) \subseteq \mathbb{P}(V)$, and we call it the *rank of* U *in* G, although we will not make use of this in our argument.

We find it useful to consider the surjective map

$$\Phi : V \times K \xrightarrow{(v,\lambda)\mapsto T_v[\lambda]} \{\text{symplectic transvections in } \mathrm{Sp}(V)\}.$$

The multiplicative group $K^\times$ acts on $V \times K$ via $x(v,\lambda) := (xv, x^{-2}\lambda)$. Passing to the quotient modulo this action yields a bijection

$$(V \setminus \{0\} \times K)/K^\times \xrightarrow{(v,\lambda)\mapsto T_v[\lambda]} \{\text{nontrivial symplectic transvections in } \mathrm{Sp}(V)\}.$$

When we consider the first projection $\pi_V : V \times K \twoheadrightarrow V$ modulo the action of $K^\times$ we obtain

$$\pi_V : (V \setminus \{0\} \times K)/K^\times \twoheadrightarrow \mathbb{P}(V),$$

which corresponds to sending a nontrivial transvection to its centre. Let W be a K-subspace of V. Then Φ gives a bijection

$$(W \setminus \{0\} \times K)/K^\times \xrightarrow{(v,\lambda)\mapsto T_v[\lambda]} \{\text{nontrivial symplectic transvections in } \mathrm{Sp}(V) \text{ with centre in } W\}.$$

Let L be a subfield of K. We call an L-vector space $W_L \subseteq V$ *L-rational* if $\dim_K W_K = \dim_L W_L$ with $W_K := \langle W_L \rangle_K$ and $\langle \cdot, \cdot \rangle$ restricted to $W_L \times W_L$ takes values in L. An L-vector space $W_L \subseteq V$ is called *(L,G)-rational* if W_L is L-rational and Φ induces a bijection

$$(W_L \setminus \{0\} \times L)/L^\times \xrightarrow{(v,\lambda)\mapsto T_v[\lambda]} G \cap \{\text{nontrivial sympl. transvections in } \mathrm{Sp}(V) \text{ with centre in } W_K\}.$$

Note that $(W_L \setminus \{0\} \times L)/L^\times$ is naturally a subset of $(W_K \setminus \{0\} \times K)/K^\times$. A K-subspace $W \subseteq V$ is called *(L,G)-rationalisable* if there exists an (L,G)-rational W_L with $W_K = W$. We speak of an (L,G)-rational symplectic subspace W_L if it is (L,G)-rational and symplectic in the sense that the restricted pairing is non-degenerate on W_L. Let H_L and I_L be two (L,G)-rational symplectic subspaces of V. We say that *H_L and I_L are (L,G)-linked* if there is $0 \neq h \in H_L$ and $0 \neq w \in I_L$ such that $h + w \in \mathcal{L}(G)$.

2.2 Strategy

Now that we have set up all notation, we will describe the strategy behind the proof of Theorem 1.1, as a service for the reader.

If one is not in case 1., then there are 'many' transvections in G, as otherwise the K-span of $\mathcal{L}(G)$ would be a proper subspace of V stabilised by G. The presence of 'many' transvection is used first in order to show the existence of a subfield $L \subseteq K$ and an (L,G)-rational symplectic plane $H_L \subseteq V$. For this it is necessary to replace G by one of its conjugates inside $\mathrm{GSp}(V)$. The main ingredient for the existence of (L,G)-rational symplectic planes, which is treated in Section 2.4, is Dickson's classification of the finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$.

The next main step is to show that two (L,G)-linked symplectic spaces in V can be merged into a single one. This is the main result of Section 2.5. The main input is a result of Wagner for transvections in three dimensional vector spaces.

The merging results are applied to extend the (L, G)-rational symplectic plane further, using again the existence of 'many' transvections. We obtain a maximal (L, G)-rational symplectic space $I_L \subseteq V$ in the sense that $\mathcal{L}(G) \subset I_K \cup I_K^{\perp}$, which is proved in Section 2.6. The proof of Theorem 1.1 can be deduced from this (see Section 2.7) because either I_K equals V, that is the huge image case, or translating I_K by elements of G gives the decomposition in case 2.

2.3 Simple properties

We use the notation from the Introduction. In this subsection we list some simple lemmas illustrating and characterising the definitions made above.

Lemma 2.1. *Let $v \in \mathcal{L}(G)$. Then $\langle v \rangle_L$ is an (L, G)-rational line if and only if $\mathcal{P}_v(G) = L$.*

Proof. This follows immediately from that fact that all transvections with centre $\langle v \rangle_K$ can be written uniquely as $T_v[\lambda]$ for some $\lambda \in K$. □

Lemma 2.2. *Let $W_L \subseteq V$ be an (L, G)-rational space and U_L an L-vector subspace of W_L. Then U_L is also (L, G)-rational.*

Proof. We first give two general statements about L-rational subspaces. Let $u_1, \ldots, u_d$ be an L-basis of U_L and extend it by $w_1, \ldots, w_e$ to an L-basis of W_L. As W_L is L-rational, the chosen vectors remain linearly independent over K, and, hence, U_L is L-rational. Moreover, we see, e.g. by writing down elements in the chosen basis, that $W_L \cap U_K = U_L$.

It is clear that Φ sends elements in $(U_L \times L)/L^{\times}$ to symplectic transvections in G with centres in U_K. Conversely, let $T_v[\lambda]$ be such a transvection. As W_L is (L, G)-rational, $T_v[\lambda] = T_u[\mu]$ with some $u \in W_L$ and $\mu \in L$. Due to $W_L \cap U_K = U_L$, we have $u \in U_L$ and the tuple (u, μ) lies in $U_L \times L$. □

Lemma 2.3. *Let $W_L \subseteq V$ be an L-rational subspace of V. Then the following assertions are equivalent:*

(i) W_L is (L, G)-rational.

(ii) (a) $T_{W_L}[L] := \{T_v[\lambda] \mid \lambda \in L,\ v \in W_L\} \subseteq G$ and

(b) for each $U \in \mathcal{L}(G) \subseteq \mathbb{P}(V)$ with $U \subseteq W_K$ there is a $u \in U \cap W_L$ such that $\mathcal{P}_u(G) = L$ (i.e. $\langle u \rangle_L$ is an (L, G)-rational line contained in U by Lemma 2.1).

Proof. '(i) $\Rightarrow$ (ii):' Note that (a) is clear. For (b), let $U \in \mathcal{L}(G)$ with $U \subseteq W_K$. Hence, there is $u \in U$ and $\lambda \in K^{\times}$ with $T_u[\lambda] \in G$. As W_L is (L, G)-rational, we may assume that $u \in W_L$ and $\lambda \in L$. Lemma 2.2 implies that $\langle u \rangle_L$ is an (L, G)-rational line.

'(ii) $\Rightarrow$ (i):' Denote by ι the injection $(W_L \setminus \{0\} \times L)/L^{\times} \hookrightarrow (W_K \setminus \{0\} \times K)/K^{\times}$. By (a), the image of $\Phi \circ \iota$ lies in G. It remains to prove the surjectivity of this map onto the symplectic transvections of G with centres in W_K. Let $T_v[\lambda]$ be one such. Take $U = \langle v \rangle_K$. By (b), there is

$v_0 \in U$ such that $U_L = \langle v_0 \rangle_L \subseteq W_L$ is an (L, G)-rational line. In particular, $T_v[\lambda] = T_{v_0}[\mu]$ with some $\mu \in L$, finishing the proof. □

Lemma 2.4. *Let $A \in \mathrm{GSp}(V)$ with multiplier $\alpha \in K^\times$. Then $AT_v[\lambda]A^{-1} = T_{Av}[\frac{\lambda}{\alpha}]$. In particular, the notion of (L, G)-rationality is not stable under conjugation.*

Proof. For all $w \in V$, $AT_v[\lambda]A^{-1}(w) = A(A^{-1}w + \lambda(A^{-1}w \bullet v)v) = w + \lambda(A^{-1}w \bullet v)Av$. Since A has multiplier α, $w \bullet Av = \alpha(A^{-1}w \bullet v)$, hence $AT_v[\lambda]A^{-1}(w) = w + \frac{\lambda}{\alpha}(w \bullet Av)Av = T_{Av}[\frac{\lambda}{\alpha}](w)$. □

Lemma 2.5. *The group G maps $\mathcal{L}(G)$ into itself.*

Proof. Let $g \in G$ and $w \in \mathcal{L}(G)$, say $T_w[\lambda] \in G$. Then by Lemma 2.4 we have $gT_w[\lambda]g^{-1} = T_{gw}[\frac{\lambda}{\alpha}]$, where α is the multiplier of g. Hence, $g(w) \in \mathcal{L}(G)$. □

The following lemma shows that the natural projection yields a bijection between transvections in the symplectic group and their images in the projective symplectic group.

Lemma 2.6. *Let V be a symplectic K-vector space, $0 \neq u_1, u_2 \in V$. If $T_{u_1}[\lambda_1]^{-1}T_{u_2}[\lambda_2] \in \{a \cdot \mathrm{Id} : a \in K^\times\}$, then $T_{u_1}[\lambda_1] = T_{u_2}[\lambda_2]$.*

Proof. Assume $T_{u_1}[\lambda_1]^{-1}T_{u_2}[\lambda_2] = a\mathrm{Id}$. Then for all $v \in V$, $T_{u_2}[\lambda_2](v) - T_{u_1}[\lambda_1](av) = 0$. In particular, taking $v = u_1$, $T_{u_2}[\lambda_2](u_1) - T_{u_1}[\lambda_1](au_1) = u_1 + \lambda_2(u_1 \bullet u_2)u_2 - au_1 = 0$, hence either u_1 and u_2 are linearly dependent or $a = 1$ (thus both transvections coincide). Assume then that $u_2 = bu_1$ for some $b \in K^\times$. Then for all $v \in V$ we have $T_{bu_1}[\lambda_2](v) - T_{u_1}[\lambda_1](av) = v + \lambda_2 b^2(v \bullet u_1)u_1 - av - \lambda_1 a(v \bullet u_1)u_1 = (a-1)v + (\lambda_2 b^2 - a\lambda_1)(v \bullet u_1)u_1 = 0$. Choosing v linearly independent from u_1, we obtain $a = 1$, as we wished to prove. □

2.4 Existence of (L, G)-rational symplectic planes

Let, as before, K be a finite field of characteristic ℓ, V a n-dimensional symplectic K-vector space and $G \subseteq \mathrm{GSp}(V)$ a subgroup. We will now prove the existence of (L, G)-rational symplectic planes if there are two transvections in G with nonorthogonal directions.

Note that any additive subgroup $H \subseteq K$ can appear as a parameter group of a direction. Just take G to be the subgroup of $\mathrm{GSp}(V)$ generated by the transvections in one fixed direction with parameters in H. It might seem surprising that the existence of two nonorthogonal centres forces the parameter group to be the additive group of a subfield L of K (up to multiplication by a fixed scalar). This is the contents of Proposition 2.11, which is one of the main ingredients for this article. This proposition, in turn, is based on Proposition 2.7, going back to Mitchell (cf. [Mit11]). To make this exposition self-contained we also include a proof of it, which essentially relies on Dickson's classification of the finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$. Recall that an *elation* is the image in $\mathrm{PGL}(V)$ of a transvection in $\mathrm{GL}(V)$.

Proposition 2.7. *Let V be a 2-dimensional K-vector space with basis $\{e_1, e_2\}$ and $\Gamma \subseteq \mathrm{PGL}(V)$ a subgroup that contains two nontrivial elations whose centers U_1 and U_2 are different. Let ℓ^m be the order of an ℓ-Sylow subgroup of Γ.*

Then K contains a subfield L with ℓ^m elements. Moreover, there exists $A \in \mathrm{PGL}_2(K)$ such that $AU_1 = \langle e_1 \rangle_K$, $AU_2 = \langle e_2 \rangle_K$, and $A\Gamma A^{-1}$ is either $\mathrm{PGL}(V_L)$ or $\mathrm{PSL}(V_L)$, where $V_L = \langle e_1, e_2 \rangle_L$.

Proof. Since there are two elations τ_1 and τ_2 with independent directions U_1 and U_2, Dickson's classification of subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ (Section 260 of [Dic58]) implies that there is $B \in \mathrm{PGL}_2(K)$ such that $B\Gamma B^{-1}$ is either $\mathrm{PGL}(V_L)$ or $\mathrm{PSL}(V_L)$, where L is a subfield of K with ℓ^m elements. By Lemma 2.4, the direction of $B\tau_i B^{-1}$ is BU_i for $i = 1, 2$ and the lines BU_i are of the form $\langle d_i \rangle_K$ with $d_i \in V_L$ for $i = 1, 2$. As $\mathrm{PSL}(V_L)$ acts transitively on V_L, there is $C \in \mathrm{PSL}(V_L)$ such that $CU_1 = \langle e_1 \rangle_K$ and $CU_2 = \langle e_2 \rangle_K$. Setting $A := CB$ yields the proposition. □

Although the preceding proposition is quite simple, the very important consequence it has is that the conjugated elations $A\tau_i A^{-1}$ both have direction vectors that can be defined over the same L-rational plane.

Lemma 2.8. *Let V be a 2-dimensional K-vector space, $G \subseteq \mathrm{GL}(V)$ containing two transvections with linearly independent directions U_1 and U_2. Let ℓ^m be the order of any ℓ-Sylow subgroup of G.*

Then K contains a subfield L with ℓ^m elements and there are $A \in \mathrm{GL}(V)$ and an (L, AGA^{-1})-rational plane $V_L \subseteq V$. Moreover, A can be chosen such that $AU_i = U_i$ for $i = 1, 2$. Furthermore, if $u_1 \in U_1$ and $u_2 \in U_2$ are such that $u_1 \bullet u_2 \in L^\times$, then V_L can be chosen to be $\langle u_1, u_2 \rangle_L$.

Proof. We apply Proposition 2.7 with $e_1 = u_1$, $e_2 = u_2$, and Γ the image of G in $\mathrm{PGL}(V)$, and obtain $A \in \mathrm{GL}(V)$ (any lift of the matrix provided by the proposition) such that $A\Gamma A^{-1}$ equals $\mathrm{PSL}(V_L)$ or $\mathrm{PGL}(V_L)$ for the L-rational plane $V_L = \langle u_1, u_2 \rangle_L \subseteq V$, and $AU_i = U_i$ for $i = 1, 2$. For $\mathrm{PSL}(V_L)$ and $\mathrm{PGL}(V_L)$ it is true that the elations contained in them are precisely the images of $T_v[\lambda]$ for $v \in V_L$ and $\lambda \in L$.

First, we know that all such $T_v[\lambda]$ are contained in $\mathrm{SL}(V_L)$ and, thus, in AGA^{-1} (since $A\Gamma A^{-1}$ is $\mathrm{PSL}(V_L)$ or $\mathrm{PGL}(V_L)$). Second, by Lemma 2.6 the image of $T_v[\lambda]$ in $A\Gamma A^{-1}$ has a unique lift to a transvection in $\mathrm{SL}(V_L) \subseteq AGA^{-1}$, namely $T_v[\lambda]$. This proves that the transvections of AGA^{-1} are precisely the $T_v[\lambda]$ for $v \in V_L$ and $\lambda \in L$. Hence, V_L is an (L, AGA^{-1})-rational plane. □

Lemma 2.9. *Let $U_1, U_2 \in \mathcal{L}(G)$ be such that $H = U_1 \oplus U_2$ is a symplectic plane in V. By G_0 we denote the subgroup $\{g \in G \mid g(H) \subseteq H\}$ and by $G|_H$ the restrictions of the elements of G_0 to H.*

Then $\mathcal{L}(G|_H) \subseteq \mathcal{L}(G)$ (under the inclusion $\mathbb{P}(H) \subseteq \mathbb{P}(V)$).

Proof. Let $\tau_i \in G$ be transvections with directions U_i for $i = 1, 2$. Clearly, $\tau_1, \tau_2 \in G_0$ and their restrictions to H are symplectic transvections with the same directions. Consequently, Lemma 2.8 provides us with $A \in \mathrm{GL}(H)$ and an (L, AGA^{-1})-rational plane $H_L \subseteq H$.

Let $U \in \mathcal{L}(G|_H)$. This means that there is $g \in G_0$ such that $g|_H$ is a transvection with direction U, so that $Ag|_H A^{-1}$ is a transvection in $AG|_H A^{-1}$ with direction AU by Lemma 2.4. As H_L

is $(L, AG|_H A^{-1})$-rational, all transvections $T_v[\lambda]$ for $v \in H_L$ and $\lambda \in L$ lie in $AG|_H A^{-1}$, whence $AG|_H A^{-1}$ contains $\mathrm{SL}(H_L)$. Consequently, there is $h \in AG|_H A^{-1}$ such that $hAU = AU_1$. But $A^{-1}hA \in G|_H$, whence there is $\gamma \in G_0$ with restriction to H equal to $A^{-1}hA$. As $\gamma H \subseteq H$, it follows that $\gamma U = \gamma|_H U = A^{-1}hAU = U_1$. Now, $\gamma^{-1}\tau_1\gamma$ is a transvection in G with centre $\gamma^{-1}U_1 = U$, showing $U \in \mathcal{L}(G)$. □

Corollary 2.10. *Let $U_1, U_2 \in \mathcal{L}(G)$ be such that $H = U_1 \oplus U_2$ is a symplectic plane in V. By G_0 we denote the subgroup $\{g \in G \mid g(H) \subseteq H\}$ and by $G|_H$ the restrictions of the elements of G_0 to H. Then the transvections of $G|_H$ are the restrictions to H of the transvections of G with centre in H.*

Proof. Let T be the subgroup of G generated by the transvections of G with centre in H. We can naturally identify T with $T|_H$. Let U be the subgroup of $G|_H$ generated by the transvections of $G|_H$. We have that $T|_H \subset U$.

Applying Lemma 2.8 to the K-vector space H and the subgroup $U \subset \mathrm{GL}(H)$, there exists a subfield $L \subset K$, and an L-rational plane H_L such that U is conjugate to $\mathrm{SL}(H_L)$, hence $U \simeq \mathrm{SL}_2(L)$. Applying Lemma 2.8 to the K-vector space H and the subgroup $T|_H$, we obtain a subfield $L' \subset K$, and an L'-rational plane $H_{L'}$ such that $T|_H$ is conjugate to $\mathrm{SL}(H_{L'})$, hence $H \simeq \mathrm{SL}_2(L')$. But $\mathcal{L}(T|_H) = \mathcal{L}(G) \cap H = \mathcal{L}(G|_H) = \mathcal{L}(U)$ by Lemma 2.9, whence $L = L'$ and the cardinalities of U and $T|_H$ coincide. Therefore they are equal. □

Proposition 2.11. *Let $U_1, U_2 \in \mathcal{L}(G) \subseteq \mathbb{P}(V)$ which are not orthogonal. Then there exist a subfield $L \leq K$, $A \in \mathrm{GSp}(V)$, and an L-rational symplectic plane H_L such that $AU_1 \subseteq H_K$, $AU_2 \subseteq H_K$ and such that H_L is (L, AGA^{-1})-rational. Moreover, if we fix $u_1 \in U_1$, $u_2 \in U_2$ such that $u_1 \bullet u_2 \in L^\times$, we can choose $H_L = \langle u_1, u_2 \rangle_L$ and A satisfying $AU_1 = U_1$, $AU_2 = U_2$.*

Proof. Let $H = U_1 \oplus U_2$ and note that this is a symplectic plane. Define G_0 and $G|_H$ as in Lemma 2.9. Lemma 2.8 provides us with $B \in \mathrm{GL}(H)$ such that $BU_i = U_i$ for $i = 1, 2$ and such that $H_L = \langle u_1, u_2 \rangle_L$ is an $(L, BG|_H B^{-1})$-rational plane. We choose $A \in \mathrm{GSp}(V)$ such that $AH \subseteq H$ and $A|_H = B$ (this is possible as any symplectic basis of H can be extended to a symplectic basis of V). We want to prove that H_L is an (L, AGA^{-1})-rational symplectic plane in V.

And, indeed, by Corollary 2.10, the nontrivial transvections of AGA^{-1} with direction in H coincide with the nontrivial transvections of $BG|_H B^{-1}$, which in turn correspond bijectively to $(H_L \setminus \{0\} \times L)/L$.

□

Note that Theorem 1.1 is independent of conjugating G inside $\mathrm{Sp}(V)$. Hence, we will henceforth work with (L, G)-rational symplectic spaces (instead of (L, AGA^{-1})-rational ones).

Corollary 2.12. *(a) Let H_L be an L-rational plane which contains an (L, G)-rational line $U_{1,L}$ as well as an L-rational line $U_{2,L}$ not orthogonal to $U_{1,L}$ with $U_{2,K} \in \mathcal{L}(G)$.*

Then H_L is an (L, G)-rational symplectic plane.

(b) Let $U_{1,L} = \langle u_1 \rangle_L$ be an (L, G)-rational line and $U_2 = \langle u_2 \rangle_K \in \mathcal{L}(G)$ such that $u_1 \bullet u_2 \in L^\times$.

Then $\langle u_1, u_2 \rangle_L$ is an (L, G)-rational symplectic plane.

Proof. (a) Fix $u_1 \in U_{1,L}$ and $u_2 \in U_{2,L}$ such that $u_1 \bullet u_2 = 1$, and call $W_L = \langle u_1, u_2 \rangle_L$. Apply Proposition 2.11: we get $L \subseteq K$ and $A \in \mathrm{GSp}(V)$ such that $\langle AU_{1,L} \rangle_K = \langle u_1 \rangle_K$, $AU_2 = \langle u_2 \rangle_K$ and W_L is (L, AGA^{-1})-rational. Let $a_1, a_2 \in K^\times$ be such that $Au_1 = a_1 u_1$ and $Au_2 = a_2 u_2$. The proof will follow three steps: we will first see that $\mathcal{P}_{u_2}(G) = L$, then we will see that H_L satisfies Lemma 2.3-(ii)(a) and finally we will see that H_L satisfies Lemma 2.3-(ii)(b).

Let α be the multiplier of A. First note the following equality between α, a_1 and a_2:

$$1 = u_1 \bullet u_2 = \frac{1}{\alpha}(Au_1 \bullet Au_2) = \frac{1}{\alpha}(a_1 u_1 \bullet a_2 u_2) = \frac{a_1 a_2}{\alpha}.$$

Recall that $\mathcal{P}_{av}(G) = \frac{1}{a^2}\mathcal{P}_v(G)$, and, from Lemma 2.4 it follows that $\mathcal{P}_{Av}(AGA^{-1}) = \frac{1}{\alpha}\mathcal{P}_v(G)$.

On the one hand, since $U_{1,L}$ is (L, G)-rational and $u_1 \in U_{1,L}$, we know that $\mathcal{P}_{u_1}(G) = L$ by Lemma 2.1. On the other hand, since $\langle u_1 \rangle_L$ is (L, AGA^{-1})-rational, $\mathcal{P}_{u_1}(AGA^{-1}) = L$, hence $\mathcal{P}_{u_1}(G) = \frac{\alpha}{a_1^2}L$. We thus have $\frac{\alpha}{a_1^2} \in L$. Moreover, since $\langle u_2 \rangle_L$ is (L, AGA^{-1})-rational (e.g. using Lemma 2.2), we have that $\mathcal{P}_{u_2}(AGA^{-1}) = L$, hence $\mathcal{P}_{u_2}(G) = \frac{\alpha}{a_2^2}L = \frac{a_1^2\alpha}{\alpha^2}L = \frac{a_1^2}{\alpha}L = L$. This proves that $\langle u_2 \rangle_L$ is (L, G)-rational by Lemma 2.1.

Next we will see that $T_{H_L}[L] \subseteq G$. Let $b_1, b_2 \in L$ with $b_1 \neq 0$ and $\lambda \in L^\times$. Consider the transvection $T_{b_1u_1+b_2u_2}[\lambda]$. We want to prove that it belongs to G. We compute

$$AT_{b_1u_1+b_2u_2}[\lambda]A^{-1} = T_{A(b_1u_1+b_2u_2)}[\frac{\lambda}{\alpha}] = T_{b_1a_1u_1+b_2a_2u_2}[\frac{\lambda}{\alpha}] = T_{u_1+\frac{b_2a_2}{b_1a_1}u_2}[\frac{b_1^2a_1^2\lambda}{\alpha}].$$

Note that since $\frac{a_1}{a_2} = \frac{a_1^2}{\alpha} \in L$ and since $W_L = \langle u_1, u_2 \rangle_L$ is (L, AGA^{-1})-rational, it follows that $AT_{b_1u_1+b_2u_2}[\lambda]A^{-1} \in AGA^{-1}$, and therefore $T_{b_1u_1+b_2u_2}[\lambda] \in G$. Note that the same conclusion is valid for $b_1 = 0$ as $\langle u_2 \rangle_L$ is (L, G)-rational.

Finally it remains to see that if $U \in \mathcal{L}(G) \cap \langle H_L \rangle_K$, then there is $u \in U \cap H_L$ with $\mathcal{P}_u(G) = L$. Assume that $U \in \mathcal{L}(G) \cap \langle H_L \rangle_K$. Since we have seen that $\langle u_2 \rangle_L$ is (L, G)-rational, we can assume that $U \neq \langle u_2 \rangle_K$. Therefore we can choose an element $v \in U$ with $v = u_1 + bu_2$, for some $b \in K$. It suffices to show that $b \in L$. Let $T_v[\lambda] \in G$ be a transvection with direction U. Then computing $AT_v[\lambda]A^{-1}$ as above, we get that $AT_v[\lambda]A^{-1} = T_{u_1+\frac{ba_2}{a_1}u_2}[\frac{a_1^2\lambda}{\alpha}]$ is a transvection with direction in $\mathcal{L}(AGA^{-1}) \cap W_L$, hence the (L, AGA^{-1})-rationality of W_L implies that $b \in L$.

(b) follows from (a) by observing that the condition $u_1 \bullet u_2 \in L^\times$ ensures that $\langle u_1, u_2 \rangle_L$ is an L-rational symplectic plane. □

The next corollary says that the translate of each vector in an (L, G)-rational symplectic space by some orthogonal vector w is the centre of a transvection if this is the case for one of them.

Corollary 2.13. *Let $H_L \subseteq V$ be an (L, G)-rational symplectic space. Let $w \in H_K^\perp$ and $0 \neq h \in H_L$ such that $\langle h + w \rangle_K \in \mathcal{L}(G)$. Then $\langle h_1 + w \rangle_L$ is an (L, G)-rational line for all $0 \neq h_1 \in H_L$.*

Proof. Assume first that H_L is a plane. Let $\hat{h} \in H_L$ with $\hat{h} \bullet h = 1$ (hence $H_L = \langle h, \hat{h} \rangle_L$). As $\langle \hat{h} \rangle_L$ is an (L,G)-rational line and $\hat{h} \bullet (h+w) = 1$, it follows that $\langle \hat{h}, h+w \rangle_L$ is an (L,G)-rational plane by Corollary 2.12. Consequently, for all $\mu \in L$ we have that $\langle \mu\hat{h} + h + w \rangle_L$ is an (L,G)-rational line. Let now $\mu \in L^\times$. Then $(\mu\hat{h} + h + w) \bullet h = \mu \neq 0$, whence again by Corollary 2.12 $\langle \mu\hat{h} + h + w, h \rangle_L$ is an (L,G)-rational plane. Thus, for all $\nu \in L$ it follows that $\langle \mu\hat{h} + (\nu+1)h + w \rangle_L$ is an (L,G)-rational line. In order to get rid of the condition $\mu \neq 0$, we exchange the roles of h and $\hat{h}$, yielding the statement for planes.

To extend it to any symplectic space H_L, note that, if $h_1, h_2 \in H_L$ are nonzero elements, there exists an element $\hat{h} \in H_L$ such that $h_1 \bullet \hat{h} \neq 0$, $h_2 \bullet \hat{h} \neq 0$. Namely, let $\hat{h}_1, \hat{h}_2$ be such that $h_1 \bullet \hat{h}_1 \neq 0$, $h_2 \bullet \hat{h}_2 \neq 0$ (they exist because on H_L the symplectic pairing is nondegenerate). If $h_2 \bullet \hat{h}_1 \neq 0$ or $h_1 \bullet \hat{h}_2 \neq 0$, we are done. Otherwise $\hat{h} = \hat{h}_1 + \hat{h}_2$ satisfies the required condition.

Returning to the proof, if $h_1 \in H_L$ is nonzero, take $\hat{h} \in H_L$ such that $h \bullet \hat{h} \neq 0$ and $h_1 \bullet \hat{h} \neq 0$. First apply the Corollary to the plane $\langle h, \hat{h} \rangle_L$, yielding that $\hat{h} + w$ is an (L,G)-rational line, and then apply it to the plane $\langle \hat{h}, h_1 \rangle_L$, showing that $h_1 + w$ is an (L,G)-rational line, as required. □

In the next lemma it is important that the characteristic of K is greater than 2.

Lemma 2.14. *Let H_L be an (L,G)-rational symplectic space. Let $h, \tilde{h} \in H_L$ different from zero and let $w, \tilde{w} \in H_K^\perp$ such that $w \bullet \tilde{w} \in L^\times$ and $h + w, \tilde{h} + \tilde{w} \in \mathcal{L}(G)$.*

Then $\langle w, \tilde{w} \rangle_L$ is an (L,G)-rational symplectic plane.

Proof. By Corollary 2.13 we have that $\langle h + \tilde{w} \rangle_L$ is an (L,G)-rational line. As $(h+w) \bullet (h+\tilde{w}) = w \bullet \tilde{w} \in L^\times$, by Corollary 2.12 it follows that $\langle w - \tilde{w} \rangle_L$ is an (L,G)-rational line. Since $\langle -h - w \rangle_K \in \mathcal{L}(G)$, by Corollary 2.13 we have that $\langle -h + w \rangle_L$ is (L,G)-rational, and from $(-h+w) \bullet (h+\tilde{w}) = w \bullet \tilde{w} \in L^\times$ we conclude that $\langle w + \tilde{w} \rangle_L$ is an (L,G)-rational line. As $(w-\tilde{w}) \bullet (w+\tilde{w}) = 2w \bullet \tilde{w} \in L^\times$, we obtain that $\langle w + \tilde{w}, w - \tilde{w} \rangle_L = \langle w, \tilde{w} \rangle_L$ is an (L,G)-rational symplectic plane, as claimed. □

We now deduce that linking is an equivalence relation between mutually orthogonal spaces. Note that reflexivity and symmetry are clear and only transitivity need be shown.

Lemma 2.15. *Let H_L, I_L and J_L be mutually orthogonal (L,G)-rational symplectic subspaces of V.*

If H_L and I_L are (L,G)-linked and also I_L and J_L are (L,G)-linked, then so are H_L and J_L.

Proof. By definition there exist nonzero $h_0 \in H_L$, $i_0, i_1 \in I_L$ and $j_0 \in J_L$ such that $h_0 + i_0 \in \mathcal{L}(G)$ and $i_1 + j_0 \in \mathcal{L}(G)$. There are $\hat{h}_0 \in H_L$ and $\hat{i}_0 \in I_L$ such that $\hat{h}_0 \bullet h_0 = 1$ and $\hat{i}_0 \bullet i_0 = 1$.

By Corollary 2.13 we have, in particular, that $\langle h_0 + i_0 \rangle_L$, $\langle \hat{i}_0 + j_0 \rangle_L$ and $\langle \hat{h}_0 + (i_0 + \hat{i}_0) \rangle_L$ are (L,G)-rational lines. As $(h_0 + \hat{i}_0) \bullet (i_0 + j_0) = 1$, by Corollary 2.12 also $\langle h_0 + (i_0 + \hat{i}_0) + j_0 \rangle_L$ is (L,G)-rational. Furthermore, due to $(\hat{h}_0 + (i_0 + \hat{i}_0)) \bullet (h_0 + (i_0 + \hat{i}_0) + j_0) = 1$, it follows that $\langle (h_0 - \hat{h}_0) + j_0 \rangle_L$ is (L,G)-rational, whence H_L and J_L are (L,G)-linked. □

2.5 Merging linked orthogonal (L, G)-rational symplectic subspaces

We continue using our assumptions: K is a finite field of characteristic at least 5, $L \subseteq K$ a subfield, V a n-dimensional symplectic K-vector space, $G \subseteq \mathrm{GSp}(V)$ a subgroup. In the previous section we established the existence of (L, G)-rational symplectic planes in many cases (after allowing a conjugation of G inside $\mathrm{GSp}(V)$). In this section we aim at merging (L, G)-linked (L, G)-rational symplectic planes into (L, G)-rational symplectic subspaces.

It is important to remark that no new conjugation of G is required. The only conjugation that is needed is the one from the previous section in order to have an (L, G)-rational plane to start from.

Lemma 2.16. *Let H_L and I_L be two (L, G)-rational symplectic subspaces of V which are (L, G)-linked. Suppose that H_L and I_L are orthogonal to each other. Then all lines in $H_L \oplus I_L$ are (L, G)-rational.*

Proof. The (L, G)-linkage implies the existence of $h_1 \in H_L$ and $w_1 \in I_L$ such that $\langle h_1 + w_1 \rangle_K \in \mathcal{L}(G)$. By Corollary 2.13 $\langle h + w_1 \rangle_L$ is an (L, G)-rational line for all $h \in H_L$. The same reasoning now gives that $\langle h + w \rangle_L$ is an (L, G)-rational line for all $h \in H_L$ and all $w \in I_L$. □

In view of Lemma 2.3 the above is (ii)(a). In order to obtain (ii)(b), we need to invoke a result of Wagner.

Proposition 2.17. *Let V be a 3-dimensional vector space over a finite field K of characteristic $\ell \geq 5$, and let $G \subseteq \mathrm{SL}(V)$ be a group of transformations fixing a 1-dimensional vector space U. Let U_1, U_2, U_3 be three distinct centres of transvections in G such that $U \not\subseteq U_1 \oplus U_2$ and $U \neq U_3$. Then $(U_1 \oplus U_2) \cap (U \oplus U_3)$ is the centre of a transvection of G.*

Proof. This is Theorem 3.1-(a) of [Wag74]. It is stated in a different terminology from ours. But, note that finite desarguian projective planes correspond to usual projective planes $\mathbb{P}(V)$, where V is a 3-dimensional vector space over a finite field (see Section 1.4, 5 of [Dem97], p. 28), and collineations of such planes correspond to linear maps (cf. Section 1.4, 10 of [Dem97], p. 31). □

Proposition 2.18. *Let $U_1, U_2, U_3 \in \mathcal{L}(G)$ and $W = U_1 + U_2 + U_3$. Assume $\dim W = 3$, U_1 and U_2 not orthogonal and let U be a line in $W \cap W^\perp$ which is linearly independent from U_3 and is not contained in $U_1 \oplus U_2$. Then $(U_1 \oplus U_2) \cap (U \oplus U_3)$ is a line in $\mathcal{L}(G)$.*

Proof. Fix transvections $T_i \in G$ with centre U_i, $i = 1, 2, 3$. These transvections fix W; let $H \subseteq \mathrm{SL}(W)$ be the group generated by the restrictions of the T_i to W. The condition $U \subseteq W^\perp$ guarantees that the T_i fix U pointwise. Note that furthermore $U \neq U_3$ and $U \not\subseteq U_1 \oplus U_2$. We can apply Proposition 2.17, and conclude that $(U_1 \oplus U_2) \cap (U \oplus U_3)$ is the centre of a transvection T of H. This transvection fixes the symplectic plane $U_1 \oplus U_2$. Call T_0 the restriction of T to this plane. It is a nontrivial transvection (since no line of $U_1 \oplus U_2$ can be orthogonal to all $U_1 \oplus U_2$). Hence by Lemma 2.9 the line $(U_1 \oplus U_2) \cap (U \oplus U_3)$ belongs to $\mathcal{L}(G)$. □

We now deduce rationality statements from it.

Corollary 2.19. *Let H_L be an (L,G)-rational symplectic plane and U_3 and U_4 be linearly independent lines not contained in H_K. Assume $U_4 \subseteq H_K \oplus U_3$ is orthogonal to H_K and to U_3 and assume that $U_3 \in \mathcal{L}(G)$.*

Then the intersection $H_K \cap (U_3 \oplus U_4) = I_K$ for some line $I_L \subseteq H_L$.

Proof. Choose two (L,G)-rational lines $U_{1,L}$ and $U_{2,L}$ such that $H_L = U_{1,L} \oplus U_{2,L}$. With $U = U_4$ we can apply Proposition 2.18 in order to obtain that $I := H_K \cap (U_3 \oplus U_4)$ is a line in $\mathcal{L}(G)$ contained in H_K. As H_L is (L,G)-rational, it follows that I is (L,G)-rationalisable. □

Corollary 2.20. *Let $H_L \subseteq V$ be an (L,G)-rational symplectic space. Let $h + w \in \mathcal{L}(G)$ with $0 \neq h \in H_K$ and $w \in H_K^\perp$. Then $h \in \mathcal{L}(G)$. In particular, $\langle h \rangle_K$ is an (L,G)-rationalisable line, i.e. there is $\mu \in K^\times$ such that $\mu h \in H_L$.*

Proof. If necessary replacing H_L by any (L,G)-rational plane contained in H_L, we may without loss of generality assume that H_L is an (L,G)-rational plane. Let $y := h + w$. If $w = 0$, the claim follows from the (L,G)-rationality of H_L. Hence, we suppose $w \neq 0$. Then $U_3 := \langle y \rangle_K$ is not contained in H_K. Note that w is perpendicular to U_3 and to H_K, and $w \in H_k \oplus \langle y \rangle_K$. Hence, Corollary 2.19 gives that the intersection $H_K \cap (U_3 \oplus \langle w \rangle_K) = \langle h \rangle_K$ is in $\mathcal{L}(G)$. □

Corollary 2.20 gives the rationalisability of a line. In order to actually find a direction vector for a parameter in L, we need something extra to rigidify the situation. For this, we now take a second link which is sufficiently different from the first link.

Corollary 2.21. *Let $H_L \subseteq V$ be an (L,G)-rational symplectic space. Let $0 \neq \tilde{h} \in H_K$ and $\tilde{w} \in H_K^\perp$ such that $\tilde{h} + \tilde{w} \in \mathcal{L}(G)$. Suppose that there are nonzero $h \in H_L$ and $w \in H_K^\perp$ such that $h + w \in \mathcal{L}(G)$ and $w \bullet \tilde{w} \in L^\times$.*

Then $\tilde{h} \in H_L$.

Proof. By Corollary 2.20 there is some $\beta \in K^\times$ such that $\beta\tilde{h} \in H_L$. We want to show $\beta \in L$. By Corollary 2.13 we may assume that $h \bullet \tilde{h} \neq 0$, more precisely, $h \bullet (\beta\tilde{h}) = 1$; and we have furthermore that $\langle h + w \rangle_L$ is an (L,G)-rational line. By Corollary 2.12 (b), $\langle h, \beta\tilde{h} \rangle_L$ is an (L,G)-rational symplectic plane contained in H_L. Let $c := w \bullet \tilde{w} \in L^\times$. We have

$$(h + w) \bullet (\tilde{h} + \tilde{w}) = h \bullet \tilde{h} + w \bullet \tilde{w} = \frac{1}{\beta} + c =: \mu.$$

If $\mu = 0$, then $\beta \in L$ and we are done. Assume $\mu \neq 0$. By Corollary 2.12(b) it follows that $\langle h + w, \mu^{-1}(\tilde{h} + \tilde{w}) \rangle_L$ is an (L,G)-rational symplectic plane. Thus, $\langle h + w + \mu^{-1}(\tilde{h} + \tilde{w}) \rangle_L$ is an (L,G)-rational line. By Corollary 2.20 there is some $\nu \in K^\times$ such that $\nu(h + \mu^{-1}\tilde{h}) \in H_L$. Consequently, $\nu \in L^\times$, whence $\mu \in L$, so that $\beta \in L$. □

The main result of this section is the following merging result.

Proposition 2.22. *Let H_L and I_L be orthogonal (L,G)-rational symplectic subspaces of V that are (L,G)-linked.*

Then $H_L \oplus I_L$ is an (L,G)-rational symplectic subspace of V.

Proof. We use Lemma 2.3. Part (ii)(a) follows directly from Lemma 2.16. We now show (ii)(b). Let $h + w \in \mathcal{L}(G)$ with nonzero $h \in H_K$ and $w \in I_K$ be given. Corollary 2.20 yields $\mu, \nu \in K^\times$ such that $\mu h \in H_L$ and $\nu w \in I_L$. Let $\hat{h} \in H_L$ with $(\mu h) \bullet \hat{h} = 1$, as well as $\hat{w} \in I_L$ with $(\nu w) \bullet \hat{w} = 1$. Lemma 2.16 tells us that $\hat{h} + \hat{w} \in \mathcal{L}(G)$. Together with $(\nu h) + (\nu w) \in \mathcal{L}(G)$, Corollary 2.21 yields $\nu h \in H_L$, whence $\nu h + \nu w \in H_L \oplus I_L$. □

2.6 Extending (L,G)-rational spaces

We continue using the same notation as in the previous sections. Here, we will use the merging results in order to extend (L,G)-rational symplectic spaces.

Proposition 2.23. *Let H_L be a nonzero (L,G)-rational symplectic subspace of V. Let nonzero $h, \tilde{h} \in H_K$, $w, \tilde{w} \in H_K^\perp$ be such that $h + w, \tilde{h} + \tilde{w} \in \mathcal{L}(G)$ and $w \bullet \tilde{w} \neq 0$.*

Then there exist $\alpha, \beta \in K^\times$ such that $\langle \alpha w, \beta \tilde{w} \rangle_L$ is an (L,G)-rational symplectic plane which is (L,G)-linked with H_L.

Proof. By Corollary 2.20 we may and do assume by scaling $h + w$ that $h \in H_L$. Furthermore, we assume by scaling $\tilde{h} + \tilde{w}$ that $w \bullet \tilde{w} = 1$. Then Corollary 2.21 yields that $\tilde{h} \in H_L$. We may appeal to Lemma 2.14 yielding that $\langle w, \tilde{w} \rangle_L$ is an (L,G)-rational plane. The (L,G)-link is just given by $h + w$. □

Corollary 2.24. *Let H_L be a non-zero (L,G)-rational symplectic subspace of V. Let nonzero $h, \tilde{h} \in H_K$, $w, \tilde{w} \in H_K^\perp$ be such that $h + w, \tilde{h} + \tilde{w} \in \mathcal{L}(G)$ and $w \bullet \tilde{w} \neq 0$.*

Then there is an (L,G)-rational symplectic subspace I_L of V containing H_L and such that $I_K = \langle H_K, w, \tilde{w} \rangle_K$.

Proof. This follows directly from Propositions 2.23 and 2.22. □

Proposition 2.25. *Assume $\langle \mathcal{L}(G) \rangle_K = V$. Let H_L be a nonzero (L,G)-rational symplectic space. Let $0 \neq v \in \mathcal{L}(G) \setminus (H_K \cup H_K^\perp)$.*

Then there is an (L,G)-rational symplectic space I_L containing H_L such that $v \in I_K$.

Proof. We write $v = h + w$ with $h \in H_K$ and $w \in H_K^\perp$. Note that both h and w are nonzero by assumption. As $\langle \mathcal{L}(G) \rangle_K = V$, we may choose $\tilde{v} \in \mathcal{L}(G)$ such that $\tilde{v} \bullet w \neq 0$. We again write $\tilde{v} = \tilde{h} + \tilde{w}$ with $\tilde{h} \in H_K$ and $\tilde{w} \in H_K^\perp$.

We, moreover, want to ensure that $\tilde{h} \neq 0$. If $\tilde{h} = 0$, then we proceed as follows. Corollary 2.20 implies the existence of $\mu \in K^\times$ such that $\mu h \in H_L$. Now replace h by μh and w be μw. Then Corollary 2.13 ensures that $\langle h + w \rangle_L$ is an (L,G)-rational line. Furthermore, scale $\tilde{w}$ so that $(h +$

$w) \bullet \tilde{w} \in L^\times$, whence by Corollary 2.12 $h + w + \tilde{w} \in \mathcal{L}(G)$. We use this element as $\tilde{v}$ instead. Note that it still satisfies $\tilde{v} \bullet w \neq 0$, but now $\tilde{h} \neq 0$.

Now we are done by Corollary 2.24. □

Corollary 2.26. *Assume $\langle \mathcal{L}(G) \rangle_K = V$, and let H_L be an (L, G)-rational symplectic space.*

Then there is an (L, G)-rational symplectic space I_L containing H_L such that $\mathcal{L}(G) \subseteq I_K \cup I_K^\perp$.

Proof. Iterate Proposition 2.25. □

2.7 Proofs of group theoretic results

In this section we will finish the proofs of Theorem 1.1 and Corollaries 1.2 and 1.3.

Lemma 2.27. *Let $V = S_1 \oplus \cdots \oplus S_h$ be a decomposition of V into linearly independent, mutually orthogonal subspaces such that $\mathcal{L}(G) \subseteq S_1 \cup \cdots \cup S_h$.*

(a) If $v_1, v_2 \in \mathcal{L}(G) \cap S_1$ are such that $v_1 + v_2 \in \mathcal{L}(G)$, then for all $g \in G$ there exists an index $i \in \{1, \ldots, h\}$ such that $g(v_1)$ and $g(v_2)$ belong to the same S_i.

(b) If S_1 is (L, G)-rationalisable, then for all $g \in G$ there exists an index $i \in \{1, \ldots, h\}$ such that $gS_1 \subseteq S_i$.

Proof. (a) Assume that $g(v_1) \in S_i$ and $g(v_2) \in S_j$ with $i \neq j$. Then $g(v_1) + g(v_2) = g(v_1 + v_2) \in \mathcal{L}(G)$ satisfies $g(v_1 + v_2) \in S_i \oplus S_j$, but it neither belongs to S_i nor to S_j. This contradicts the assumption that $\mathcal{L}(G) \subseteq S_1 \cup \cdots \cup S_h$.

(b) If $S_1 = S_{1,L}$ with $S_{1,L}$ an (L, G)-rational space, we can apply (a) to an L-basis of $S_{1,L}$. □

Corollary 2.28. *Let $I_L \subseteq V$ be an (L, G)-rational symplectic subspace such that $\mathcal{L}(G) \subseteq I_K \cup I_K^\perp$ and let $g \in G$. Then either $g(I_K) = I_K$ or $g(I_K) \subseteq I_K^\perp$; in the latter case $I_K \cap g(I_K) = 0$.*

Proof. This follows from Lemma 2.27 with $S_1 = I_K$ and $S_2 = I_K^\perp$. □

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. As we assume that G contains some transvection, it follows that $\mathcal{L}(G)$ is nonempty and consequently $\langle \mathcal{L}(G) \rangle_K$ is a nonzero K-vector space stabilised by G due to Lemma 2.5. Hence, either we are in case 1. of Theorem 1.1 or $\langle \mathcal{L}(G) \rangle_K = V$, which we assume now.

From Proposition 2.11 we obtain that there is some $A \in \mathrm{GSp}(V)$, a subfield $L \leq K$ such that there is an (L, AGA^{-1})-rational symplectic plane H_L. Since the statements of Theorem 1.1 are not affected by this conjugation, we may now assume that H_L is (L, G)-rational.

From Corollary 2.26 we obtain an (L, G)-rational symplectic space $I_{1,L}$ such that $\mathcal{L}(G) \subseteq I_{1,K} \cup I_{1,K}^\perp$. If $I_{1,K} = V$, then we know due to $I_{1,L} \cong L^n$ that G contains a transvection whose direction is any vector of $I_{1,L}$. As the transvections generate the symplectic group, it follows that G contains $\mathrm{Sp}(I_{1,L}) \cong \mathrm{Sp}_n(L)$ and we are in case 3. of Theorem 1.1. Hence, suppose now that $I_{1,K} \neq V$.

Either every $g \in G$ stabilises $I_{1,K}$, and we are in case 1. and done, or there is $g \in G$ and $v \in I_{1,L}$ with $g(v) \notin I_{1,K}$. Set $I_{2,L} := gI_{1,L}$. Note that $I_{2,L} \subseteq \mathcal{L}(G)$ because of Lemma 2.4. Now we apply Corollary 2.28 to the decomposition $V = I_{1,K} \oplus I_{1,K}^{\perp}$ and obtain that $g(I_{1,K}) \subseteq I_{1,K}^{\perp}$. Moreover $\mathcal{L}(G) = \mathcal{L}(gGg^{-1}) \subseteq gI_{1,K} \cup gI_{1,K}^{\perp} = I_{2,K} \cup I_{2,K}^{\perp}$.

We now have $\mathcal{L}(G) \subseteq I_{1,K} \cup I_{2,K} \cup (I_{1,K} \oplus I_{2,K})^{\perp}$. Either $I_{1,K} \oplus I_{2,K} = V$ and $(I_{1,K} \oplus I_{2,K})^{\perp} = 0$, or there are two possibilities:

- For all $g \in G$, $gI_{1,L} \subseteq I_{1,K} \cup I_{2,K}$. If this is the case, then G fixes the space $I_{1,K} \oplus I_{2,K}$, and we are in case 1. and done.
- There exists $g \in G$, $v \in I_{1,L}$ such that $g(v) \notin I_{1,K} \cup I_{2,K}$. Set $I_{3,L} = gI_{1,L}$. Due to $\mathcal{L}(G) \subseteq I_{3,K} \cup I_{3,K}^{\perp}$, we then have $\mathcal{L}(G) \subseteq I_{1,K} \cup I_{2,K} \cup I_{3,K} \cup (I_{1,K} \oplus I_{2,K} \oplus I_{3,K})^{\perp}$.

Hence, iterating this procedure, we see that either we are in case 1., or we obtain a decomposition $V = I_{1,K} \oplus \cdots \oplus I_{h,K}$ with mutually orthogonal symplectic spaces such that $\mathcal{L}(G) \subseteq I_{1,K} \cup \cdots \cup I_{h,K}$.

Note that Lemma 2.27 implies that G respects this decomposition in the sense that for all $i \in \{1, \ldots, h\}$ there is $j \in \{1, \ldots, h\}$ such that $g(I_{i,K}) = I_{j,K}$. If the resulting action of G on the index set $\{1, \ldots, h\}$ is not transitive, then we are again in case 1., otherwise in case 2. □

Proof of Corollary 1.2. Since Γ is compact and the topology on $\overline{\mathbb{F}}_\ell$ is discrete, the image of ρ is a subgroup of $\mathrm{GSp}_n(K)$ for a certain finite field K of characteristic ℓ. Therefore one of the three possibilities of Theorem 1.1 holds for $G := \mathrm{im}(\rho)$. If the first holds, then ρ is reducible, and if the third holds, then $\mathrm{im}(\rho)$ contains a group conjugate to $\mathrm{Sp}_n(L)$ for some subfield L of K.

Assume now that the second possibility holds. We use notation as in Theorem 1.1. Let Γ' be $\{g \in \Gamma \mid \sigma_g(1) = 1\}$, the stabiliser of the first subspace. This is a closed subgroup of Γ of finite index. Choose coset representatives and write $\Gamma = \bigsqcup_{i=1}^{h'} g_i \Gamma'$. The set $\{\gamma S_1 \mid \gamma \in \Gamma\}$ contains h' elements, namely precisely the $g_i S_1$ for $i = 1, \ldots, h'$. As the action of G on the decomposition is transitive, this set is precisely $\{S_1, \ldots, S_h\}$, whence $h = h'$. Define ρ' as the restriction of ρ to Γ' acting on S_1. Then as Γ-representation we have the isomorphism

$$V \cong \bigoplus_{i=1}^{h} S_i \cong \bigoplus_{i=1}^{h} g_i S_1.$$

Proposition (10.5) of $\S 10A$ of [CR81] implies that $\rho = \mathrm{Ind}_{\Gamma'}^{\Gamma}(\rho')$. □

Proof of Corollary 1.3. Assume that G contains a subgroup conjugate (in $\mathrm{GSp}(V)$) to $\mathrm{Sp}_n(\mathbb{F}_\ell)$. In particular, G does not fix any proper subspace $S \subset V$, nor any decomposition $V = \bigoplus_{i=1}^{h} S_i$ into mutually orthogonal nonsingular symplectic subspaces. Hence by Theorem 1.1 there is a subfield L of K such that the subgroup generated by the symplectic transvections of G is conjugated (in $\mathrm{GSp}(V)$) to $\mathrm{Sp}_n(L)$. The other implication is clear. □

3 Symplectic representations with huge image

In this section we establish Theorem 1.4.

3.1 (n,p)-groups

As a generalisation of dihedral groups, in [KLS08], Khare, Larsen and Savin introduce so-called (n,p)-groups. We briefly recall some facts and some notation to be used. For the definition of (n,p)-groups we refer to [KLS08]. Let q be a prime number, and let $\mathbb{Q}_{q^n}/\mathbb{Q}_q$ be the unique unramified extension of $\mathbb{Q}_q$ of degree n (inside a fixed algebraic closure $\overline{\mathbb{Q}}_q$). Assume p is a prime such that the order of q modulo p is n. Recall that $\mathbb{Q}_{q^n}^\times \simeq \mu_{q^n-1} \times U_1 \times q^{\mathbb{Z}}$, where μ_{q^n-1} is the group of (q^n-1)-th roots of unity and U_1 the group of 1-units. Let ℓ be a prime distinct from p and q. Assuming that $p, q > n$, in [KLS08] the authors construct a character $\chi_q : \mathbb{Q}_{q^n}^\times \to \overline{\mathbb{Q}}_\ell^\times$ that satisfies the three properties of the following Lemma, which is proved in [KLS08], Section 3.1.

Lemma 3.1. *Let $\chi_q : \mathbb{Q}_{q^n}^\times \to \overline{\mathbb{Q}}_\ell^\times$ be a character satisfying:*

- *χ_q has order $2p$.*
- *$\chi_q|_{\mu_{q^n-1}\times U_1}$ has order p.*
- *$\chi_q(q) = -1$.*

This character gives rise to a character (which by abuse of notation we call also χ_q) of $G_{\mathbb{Q}_{q^n}}$ by means of the reciprocity map of local class field theory.

Let $\rho_q = \mathrm{Ind}_{G_{\mathbb{Q}_{q^n}}}^{G_{\mathbb{Q}_q}}(\chi_q)$. Then ρ_q is irreducible and symplectic (i.e., can be conjugated to take values in $\mathrm{GSp}_n(\overline{\mathbb{Q}}_\ell)$), and the image of the reduction of ρ_q in $\mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$ is an (n,p)-group.

Note that the reduction of ρ_q is $\mathrm{Ind}_{G_{\mathbb{Q}_{q^n}}}^{G_{\mathbb{Q}_q}}(\overline{\chi}_q)$, which is an irreducible representation. Here $\overline{\chi}_q$ is the composite of χ_q and the projection $\overline{\mathbb{Z}}_\ell \twoheadrightarrow \overline{\mathbb{F}}_\ell$.

3.2 Regular Galois representations

In our result we assume that our representation ρ is regular, which is defined as follows.

Definition 3.2 (Regularity)**.** *Let ℓ be a prime number, n an even natural number, V an n-dimensional vector space over $\overline{\mathbb{F}}_\ell$ endowed with a symplectic form and $\rho : G_{\mathbb{Q}_\ell} \to \mathrm{GSp}(V)$ a Galois representation, and denote by I_ℓ the inertia group at ℓ. We say that ρ is* regular *if there exists an integer s between 1 and n, and for each $i = 1, \ldots, s$, a set S_i of natural numbers in $\{0, 1, \ldots, \ell-1\}$, of cardinality r_i, with $r_1 + \cdots + r_s = n$, say $S_i = \{a_{i,1}, \ldots, a_{i,r_i}\}$, such that the cardinality of $S = S_1 \cup \cdots \cup S_s$*

equals n (i.e. all the $a_{i,j}$ are distinct) and such that, if we denote by B_i the matrix

$$B_i \sim \begin{pmatrix} \psi_{r_i}^{b_i} & & & 0 \\ & \psi_{r_i}^{b_i\ell} & & \\ & & \ddots & \\ 0 & & & \psi_{r_i}^{b_i\ell^{r_i-1}} \end{pmatrix}$$

with ψ_{r_i} our fixed choice of fundamental character of niveau r_i and $b_i = a_{i,1} + a_{i,2}\ell + \cdots + a_{i,r_i}\ell^{r_i-1}$, then

$$\rho|_{I_\ell} \sim \begin{pmatrix} \boxed{B_1} & & * \\ & \ddots & \\ 0 & & \boxed{B_s} \end{pmatrix}.$$

We will say that ρ has inertial weights at most k *if $S \subseteq \{0, 1, \ldots, k\}$. We will say that a global representation $\rho : G_{\mathbb{Q}} \to \mathrm{GSp}(V)$ is* regular *if $\rho|_{G_{\mathbb{Q}_\ell}}$ is regular.*

Lemma 3.3. *Let $\rho : G_{\mathbb{Q}_\ell} \to \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ be a Galois representation which is regular with inertial weights at most k. Assume that $\ell > kn! + 1$. Then all the $n!$-th powers of the characters on the diagonal of $\rho|_{I_\ell}$ are different.*

Proof. We use the notation of Definition 3.2. Assume we had that the $n!$-th powers of two characters of the diagonal coincide, say

$$\psi_{r_i}^{n!(c_0+c_1\ell+\cdots+c_{r_i-1}\ell^{r_i-1})} = \psi_{r_j}^{n!(d_0+d_1\ell+\cdots+d_{r_j-1}\ell^{r_j-1})},$$

where $c_0, \ldots, c_{r_i-1}, d_0, \ldots, d_{r_j-1}$ are different elements of $S_1 \cup \cdots \cup S_s$.

Let $\psi_{r_ir_j}$ be a fundamental character of niveau r_ir_j such that $\psi_{r_ir_j}^{\frac{\ell^{r_ir_j}-1}{\ell^{r_i}-1}} = \psi_{r_i}$ and $\psi_{r_ir_j}^{\frac{\ell^{r_ir_j}-1}{\ell^{r_j}-1}} = \psi_{r_j}$. We can write the equality above as

$$\psi_{r_ir_j}^{\frac{\ell^{r_ir_j}-1}{\ell^{r_i}-1}n!(c_0+c_1\ell+\cdots+c_{r_i-1}\ell^{r_i-1})} = \psi_{r_ir_j}^{\frac{\ell^{r_ir_j}-1}{\ell^{r_j}-1}n!(d_0+d_1\ell+\cdots+d_{r_j-1}\ell^{r_j-1})}.$$

In other words, $\ell^{r_ir_j} - 1$ divides the quantity

$$C_0 = |\frac{\ell^{r_ir_j}-1}{\ell^{r_i}-1}n!(c_0 + c_1\ell + \cdots + c_{r_i-1}\ell^{r_i-1}) - \frac{\ell^{r_ir_j}-1}{\ell^{r_j}-1}n!(d_0 + d_1\ell + \cdots + d_{r_j-1}\ell^{r_j-1})|.$$

Note that C_0 is nonzero because modulo ℓ it is congruent to $n!(c_0 - d_0)$, and by assumption all elements in $S_1 \cup \cdots \cup S_s$ are in different congruence classes modulo ℓ. But $|c_0 + c_1\ell + \cdots + c_{r_i-1}\ell^{r_i-1}| \leq k(1 + \ell + \cdots + \ell^{r_i-1}) = k(\ell^{r_i} - 1)/(\ell - 1)$. Analogously $|d_0 + d_1\ell + \cdots + d_{r_j-1}\ell^{r_j-1}| < k(\ell^{r_j} - 1)/(\ell - 1)$. Thus

$$\begin{aligned} C_0 &\leq \max\{|\frac{\ell^{r_ir_j}-1}{\ell^{r_i}-1}n!(c_0 + c_1\ell + \cdots + c_{r_i-1}\ell^{r_i-1})|, |\frac{\ell^{r_ir_j}-1}{\ell^{r_j}-1}n!(d_0 + d_1\ell + \cdots + d_{r_j-1}\ell^{r_j-1})|\} \\ &\leq n!k \max\{\frac{\ell^{r_ir_j}-1}{\ell^{r_i}-1}\frac{\ell^{r_i}-1}{\ell-1}, \frac{\ell^{r_ir_j}-1}{\ell^{r_j}-1}\frac{\ell^{r_j}-1}{\ell-1}\} \\ &= n!k\left(\frac{\ell^{r_ir_j}-1}{\ell-1}\right) < n!k\left(\ell^{r_ir_j-1} + 2\ell^{r_ir_j-2}\right). \end{aligned}$$

Since $\ell - 2 \geq n!k$, we have $\ell^2 - 1 > \ell^2 - 4 \geq n!k(\ell+2)$ and thus $C_0 < n!k(\ell^{r_i r_j - 1} + 2\ell^{r_i r_j - 2}) = n!k(\ell+2)\ell^{r_i r_j - 2} < \ell^{r_i r_j} - 1$. Hence $\ell^{r_i r_j} - 1$ cannot divide C_0. □

Lemma 3.4. *Let ℓ be a prime and $\beta : G_{\mathbb{Q}_\ell} \to \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ be a representation. Call V the $\overline{\mathbb{F}}_\ell$-vector space on which β acts. Then there is a basis of V such that*

$$\beta|_{I_\ell} = \begin{pmatrix} \boxed{B_1} & & * \\ & \ddots & \\ 0 & & \boxed{B_s} \end{pmatrix}$$

where each block B_i has the form

$$B_i = \begin{pmatrix} \varphi_1 & & & 0 \\ & \varphi_2 & & \\ & & \ddots & \\ 0 & & & \varphi_r \end{pmatrix},$$

for some $\varphi_1, \ldots, \varphi_r$ characters of the tame inertia group.

Proof. Consider a Jordan-Hölder series of $\beta|_{I_\ell}$; say it has s blocks, and call r_i the dimension of the i-th block as an $\overline{\mathbb{F}}_\ell$-vector space. Choose a basis of V such that the first r_1 vectors form a basis of the first block V_1, the next r_2 a basis of the first block in V/V_1, and so on. We get that $\beta|_{I_\ell}$ will have the shape

$$\beta|_{I_\ell} \sim \begin{pmatrix} \boxed{B_1} & & * \\ & \ddots & \\ 0 & & \boxed{B_s} \end{pmatrix}$$

where each B_i is a simple block, i.e., and irreducible $G_{\mathbb{Q}_\ell}$-representation. To simplify notation, let us focus on one of the blocks; call it B. According to Proposition 4 of [Ser72], the image of the wild inertia group $I_{\ell,\mathrm{w}}$ on B is trivial. Therefore, the image of I_ℓ by β is a cyclic group of order prime to ℓ (because the action factors through the pro-cyclic group I_t of tame inertia), so we can choose a new basis for V such that we have

$$B = \begin{pmatrix} \varphi_1 & & 0 \\ & \ddots & \\ 0 & & \varphi_r \end{pmatrix},$$

where the φ_j are characters of the tame inertia group I_t. □

We will now use these lemmas to study the ramification at ℓ of an induced representation under the assumption of regularity and boundedness of inertial weights.

Proposition 3.5. *Let $n, m, k \in \mathbb{N}$, let $\ell > kn! + 1$ be a prime, $K/\mathbb{Q}$ a finite extension and $\rho : G_K \to \mathrm{GL}_m(\overline{\mathbb{F}}_\ell)$ be a Galois representation and $\alpha = \mathrm{Ind}_{G_\mathbb{Q}}^{G_K} \rho$ an n-dimensional representation which is regular with inertial weights at most k. Then $K/\mathbb{Q}$ does not ramify at ℓ.*

Proof. Let us assume that $K/\mathbb{Q}$ ramifies in ℓ. Write the decomposition of (ℓ) in $K/\mathbb{Q}$ as $(\ell) = \Lambda_1^{e_1} \cdot \cdots \cdot \Lambda_s^{e_s}$, where there is at least one index i with $e_i > 1$, say $e_1 > 1$. Let w be the extension of the ℓ-adic valuation v of $\mathbb{Q}$ to K that corresponds to Λ_1. Denote by I_ℓ the inertia group of $G_{\mathbb{Q}_\ell}$ and I_w the inertia group of G_{K_w}. Let furthermore be W the m-dimensional vector space subjacent to ρ and V the n-dimensional vector space subjacent to α. Note that $V = \bigoplus_{\gamma\in\Gamma} \gamma W$, where Γ is a set of coset representatives of $G_{\mathbb{Q}}/G_K$.

Since ρ is regular, we know that there exists a vector $v \in V$ which is an eigenvector for all $\sigma \in I_\ell$ (namely the first vector of the basis from Definition 3.2). In particular, it is an eigenvector for all $\sigma \in I_w$. On the other hand, by Lemma 3.3, we know that the n characters that appear on the diagonal of $\alpha|_{I_w}$ are different (since the index $[I_\ell : I_w]|n!$). This implies that all the simultaneous eigenvectors of I_w lie in $\bigcup_{\gamma\in\Gamma} \gamma W$. Indeed, if we write $\Gamma = \{\gamma_1, \ldots, \gamma_r\}$, we can choose a Jordan-Hölder series of $\alpha|_{I_w}$ compatible with the series $\gamma_1 W \subset \gamma_1 W \oplus \gamma_2 W \subset \cdots \subset \gamma_1 W \oplus \cdots \oplus \gamma_r W = V$ and apply Lemma 3.4 to find a basis $\{v_1, \ldots, v_n\}$ of V such that the first m vectors are a basis of $\gamma_1 W$, the next m vectors or $\gamma_2 W$, and so on, and such that

$$\alpha|_{I_w} = \begin{pmatrix} \varphi_1 & & * \\ & \ddots & \\ 0 & & \varphi_n \end{pmatrix}.$$

The eigenvectors are thus the elements of this basis, which belong to $\bigcup_{\gamma\in\Gamma} \gamma W$.

Since v is a simultaenous eigenvector for all the σ in I_w, it belongs to γW for some $\gamma \in \Gamma$. Λ_1 is ramified in $K/\mathbb{Q}$, thus there exists $\sigma \in I_\ell$ which does not belong to G_K. But then $\sigma(v) = \varphi_i(v)v \in \sigma\gamma W \cap \gamma W = 0$, which is a contradiction.

□

3.3 Representations induced in two ways

We need a proposition concerning representations induced from different subgroups of a certain group G.

Proposition 3.6. *Let G be a finite group, $N \trianglelefteq G$, $H \leq G$. Assume $(G : N) = n$, and let $q > n$ be a prime. Let K be a field of characteristic coprime to $|G|$ containing all $|G|$-th roots of unity. Let S be a $K[H]$-module, $\chi : N \to K^\times$ a nontrivial character of order a power of q, and assume*

$$\rho := \mathrm{Ind}_H^G(S) = \mathrm{Ind}_N^G(\chi),$$

and furthermore ρ is an irreducible $K[G]$-module. Then $N \leq H$.

Following 7.2 of [Ser77], if G is a finite group and we are given two G-modules V_1 and V_2, we will denote by $\langle V_1, V_2\rangle_G := \dim \mathrm{Hom}_G(V_1, V_2)$. It is known (Lemma 2 of Chapter 7 of [Ser77]) that, if φ_1 and φ_2 are the characters of V_1 and V_2, then $\langle V_1, V_2\rangle_G = \langle \varphi_1, \varphi_2\rangle_G := \frac{1}{|G|} \sum_{g\in G} \varphi_1(g^{-1})\varphi_2(g)$.

Before giving the proof, we will first prove a lemma.

Lemma 3.7. *Let G be a group, $N \trianglelefteq G$ and $H \leq G$ such that $(G : H) \leq n$. Let q be a prime such that $q > n$, let K be a field of characteristic coprime to $|G|$ containing all $|G|$-th roots of unity, and let $\chi : N \to K^\times$ be a character of order a power of q which is not trivial. Then $\mathrm{Res}^N_{H\cap N}\chi$ is not trivial.*

Proof. Assume $\mathrm{Res}^N_{H\cap N}\chi$ is trivial. Then $H \cap N \leq \ker\chi$. But $\ker\chi \leq N$, and the index $(N : \ker\chi) \geq q$. Therefore $(N : H \cap N) \geq q$. But on the other hand $q > n \geq (G : H) \geq (HN : H) = (N : N \cap H)$. Contradiction. □

Proof of Proposition 3.6. Since ρ is irreducible, we have that

$$1 = \langle\rho, \rho\rangle_G = \langle \mathrm{Ind}^G_H(S), \mathrm{Ind}^G_N(\chi)\rangle_G = \langle S, \mathrm{Res}^G_H \mathrm{Ind}^G_N(\chi)\rangle_H = \cdots,$$

where in the last step we used Frobenius reciprocity. Now we apply Mackey's formula on the right hand side; note that, since N is normal, $H\backslash G/N \simeq G/(H \cdot N)$:

$$\cdots = \langle S, \bigoplus_{\gamma\in G/(H\cdot N)} \mathrm{Ind}^H_{H\cap N}\mathrm{Res}^N_{H\cap N}(\chi^\gamma)\rangle_H = \sum_{\gamma\in G/(H\cdot N)} \langle S, \mathrm{Ind}^H_{H\cap N}\mathrm{Res}^N_{H\cap N}(\chi^\gamma)\rangle_H.$$

Hence there is a unique $\gamma \in G/(H \cdot N)$ such that

$$\langle S, \mathrm{Ind}^H_{H\cap N}\mathrm{Res}^N_{H\cap N}(\chi^\gamma)\rangle_H = 1.$$

If we prove that, for all γ, $\mathrm{Ind}^H_{H\cap N}\mathrm{Res}^N_{H\cap N}(\chi^\gamma)$ is irreducible, then we will have that

$$S \simeq \mathrm{Ind}^H_{H\cap N}\mathrm{Res}^N_{H\cap N}(\chi^\gamma)$$

(for some γ), hence $\dim(S) = (H : H\cap N)$. But, on the other hand, since $\rho = \mathrm{Ind}^G_H(S) = \mathrm{Ind}^G_N(\chi)$, we have that $\dim(S) \cdot (G : H) = (G : N)$, so

$$\dim(S) = \frac{(G : HN)(HN : N)}{(G : HN)(HN : H)} = \frac{(H : N \cap H)}{(N : N \cap H)},$$

and therefore the conclusion is that $(N : N \cap H) = 1$, in other words, $N \leq H$.

Therefore to conclude we only need to see that $\mathrm{Ind}^H_{H\cap N}\mathrm{Res}^N_{H\cap N}(\chi^\gamma)$ is irreducible. Since conjugation by γ plays no role here, let us just assume $\gamma = 1$. There is a well-known criterion characterising when an induced representation is irreducible (cf. [Ser77], Proposition 23, Chapter 7). In particular, since $H\cap N$ is normal in H, we have that $\mathrm{Ind}^H_{H\cap N}\mathrm{Res}^N_{H\cap N}(\chi)$ is irreducible if and only if $\mathrm{Res}^N_{H\cap N}(\chi)$ is irreducible (which clearly holds) and, for all $h \in H/N \cap H$, $(\mathrm{Res}^N_{H\cap N}(\chi))^h$ is not isomorphic to $\mathrm{Res}^N_{H\cap N}(\chi)$.

So pick $h \in H \setminus N$. We have $(\mathrm{Res}^N_{H\cap N}(\chi))^h = \mathrm{Res}^N_{H\cap N}(\chi^h)$. Assume that $\mathrm{Res}^N_{H\cap N}(\chi^h) = \mathrm{Res}^N_{H\cap N}(\chi)$. By Lemma 3.7, it holds that $\chi = \chi^h$ as characters of N. But we know that, since $\mathrm{Ind}^G_N(\chi)$ is irreducible, for all $\sigma \in G/N$, $\chi^\sigma \neq \chi$. Now it suffices to observe that $H/(H \cap N) \hookrightarrow G/N$. □

3.4 Proofs

Finally we carry out the proof of Theorem 1.4.

Proof of Theorem 1.4. Let $G = \mathrm{Im}\rho$. Since G contains a transvection, one of the following three possibilities holds (cf. Corollary 1.2):

1. ρ is reducible.
2. There exists an open subgroup $H \subset G_{\mathbb{Q}}$, say of index h with n/h even, and a representation $\rho' : H \to \mathrm{GSp}_{n/h}(\overline{\mathbb{F}}_\ell)$ such that $\rho \simeq \mathrm{Ind}_H^{G_{\mathbb{Q}}}\rho'$.
3. The group generated by the transvections in G is conjugated (in $\mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$) to $\mathrm{Sp}_n(\mathbb{F}_{\ell^r})$ for some exponent r.

By Lemma 3.1 there is an (n,p)-group contained in G. In particular Lemma 2.1 of [KLS08] implies that G acts irreducibly on V, hence the first possibility cannot occur. To prove the theorem, it suffices to see that the second possibility does not hold.

Assume then that there exists an open subgroup $H \subset G_{\mathbb{Q}}$, say of index h with n/h even, and a representation $\rho' : H \to \mathrm{GSp}_{n/h}(\overline{\mathbb{F}}_\ell)$ such that $\rho \cong \mathrm{Ind}_H^{G_{\mathbb{Q}}}(\rho')$. Call $S_1 \subseteq V$ the subjacent space of ρ', so that we denote $\rho = \mathrm{Ind}_H^{G_{\mathbb{Q}}}(S_1)$. Recall that by assumption $\mathrm{Res}^{G_{\mathbb{Q}}}_{G_{\mathbb{Q}_q}}(\rho) = \mathrm{Ind}^{G_{\mathbb{Q}_q}}_{G_{\mathbb{Q}_{q^n}}}(\overline{\chi}_q)$. We want to compute $\mathrm{Res}^{G_{\mathbb{Q}}}_{G_{\mathbb{Q}_q}}\mathrm{Ind}_H^{G_{\mathbb{Q}}}(S_1)$. Let us apply Mackey's formula. Since we know that $\mathrm{Res}^{G_{\mathbb{Q}}}_{G_{\mathbb{Q}_q}}\mathrm{Ind}_H^{G_{\mathbb{Q}}}(S_1) = \mathrm{Ind}^{G_{\mathbb{Q}_q}}_{G_{\mathbb{Q}_{q^n}}}(\overline{\chi}_q)$ is irreducible, there can only be one summand in the formula, hence

$$\mathrm{Res}^{G_{\mathbb{Q}}}_{G_{\mathbb{Q}_q}}\mathrm{Ind}_H^{G_{\mathbb{Q}}}(S_1) = \mathrm{Ind}^{G_{\mathbb{Q}_q}}_{G_{\mathbb{Q}_q}\cap H}\mathrm{Res}^{H}_{G_{\mathbb{Q}_q}\cap H}(S_1),$$

and therefore

$$\mathrm{Ind}^{G_{\mathbb{Q}_q}}_{G_{\mathbb{Q}_q}\cap H}\mathrm{Res}^{H}_{G_{\mathbb{Q}_q}\cap H}(S_1) = \mathrm{Ind}^{G_{\mathbb{Q}_q}}_{G_{\mathbb{Q}_{q^n}}}(\overline{\chi}_q). \tag{3.1}$$

From Equation (3.1) it follows that $G_{\mathbb{Q}_{q^n}} \leq (G_{\mathbb{Q}_q} \cap H)$. We obtain this from Proposition 3.6 applied with $G = \rho(G_{\mathbb{Q}_q})$, whose order is $2np$ and, hence, prime to ℓ.

Note that, on the one hand

$$n = \dim V = \dim(\mathrm{Ind}_H^{G_{\mathbb{Q}}} S_1) = (G_{\mathbb{Q}} : H)\dim(S_1).$$

On the other hand,

$$n = \dim(\mathrm{Ind}^{G_{\mathbb{Q}_q}}_{G_{\mathbb{Q}_q}\cap H}\mathrm{Res}^{H}_{G_{\mathbb{Q}_q}\cap H}(S_1)) = (G_{\mathbb{Q}_q} : G_{\mathbb{Q}_q} \cap H)\dim S_1,$$

hence $(G_{\mathbb{Q}} : H) = (G_{\mathbb{Q}_q} : G_{\mathbb{Q}_q} \cap H)$.

Recall that $H \subset G_{\mathbb{Q}}$ is an open subgroup of finite index, say $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ for a certain number field L. Now $\mathrm{Gal}(\overline{\mathbb{Q}}/L) \cap G_{\mathbb{Q}_q} = \mathrm{Gal}(\overline{\mathbb{Q}}_q/L_{\mathfrak{q}})$, where $\mathfrak{q}$ is a certain prime of L above q and $L_{\mathfrak{q}}$

denotes the completion of L at $\mathfrak{q}$. The inclusion $G_{\mathbb{Q}_{q^n}} \leq \mathrm{Gal}(\overline{\mathbb{Q}}_q/L_{\mathfrak{q}})$ means that we have the following field diagram:

$$\begin{array}{c} \overline{\mathbb{Q}}_q \\ | \\ \mathbb{Q}_{q^n} \\ | \\ L_{\mathfrak{q}} \\ | \\ \mathbb{Q}_q \end{array}$$

and $[L_{\mathfrak{q}} : \mathbb{Q}_q] = (G_{\mathbb{Q}_q} : G_{\mathbb{Q}_q} \cap H) = (G_{\mathbb{Q}} : H) = [L : \mathbb{Q}]$, hence q is inert in $L/\mathbb{Q}$.

Let ℓ_1 be a prime dividing N_1, let $\tilde{L}/\mathbb{Q}$ be a Galois closure of $L/\mathbb{Q}$, Λ_1 a prime of $\tilde{L}$ above ℓ_1 and I_1 the inertia group of Λ_1 over $\mathbb{Q}$. Since $\gcd(|\rho(I_{\ell_1})|, n!) = 1$ and $\mathrm{Gal}(\tilde{L}/\mathbb{Q})$ has order dividing $n!$, we get that the projection of $\rho(I_1) \subseteq \rho(I_{\ell_1})$ into $\rho(G_{\mathbb{Q}})/\rho(G_{\tilde{L}})$ is trivial. That is to say, $\rho(I_1) \subset \rho(G_{\tilde{L}})$. Hence $\tilde{L}/\mathbb{Q}$ is unramified at ℓ_1 and so is $L/\mathbb{Q}$.

To sum up, we know that L can only be ramified at the primes dividing $Nq\ell$. But L cannot ramify at q since $L_{\mathfrak{q}} \subseteq \mathbb{Q}_{q^n}$ (and $\mathbb{Q}_{q^n}$ is an unramified extension of $\mathbb{Q}_q$). We just saw that L cannot ramify at the primes dividing N_1. We also know that L cannot be ramified at ℓ (cf. Proposition 3.5). Hence L only ramifies at the primes dividing N_2. By the choice of q, it is completely split in L, and at the same time inert in L. This finishes the proof of the theorem. □

Proof of Corollary 1.5. This follows from the main theorem of Part I ([AdDW12]) concerning the application to the inverse Galois problem. In order to be able to apply it, there are two things to do:

Firstly, we note that $\rho_\bullet$ is maximally induced of order p at the prime q. Secondly, the existence of a transvection in the image of $\overline{\rho}_\lambda$ together with the special shape of the representation at q allow us to conclude from Theorem 1.4 that the image of $\overline{\rho}_\lambda$ is huge for almost all λ. □

References

[AdDW12] Sara Arias-de-Reyna, Luis Dieulefait, and Gabor Wiese. Compatible systems of symplectic Galois representations and the inverse Galois problem I. Images of projective representations. *Preprint*, 2012.

[Art57] E. Artin. *Geometric algebra*. Interscience Publishers, Inc., New York-London, 1957.

[CR81] Charles W. Curtis and Irving Reiner. *Methods of representation theory. Vol. I.* John Wiley & Sons Inc., New York, 1981. With applications to finite groups and orders, Pure and Applied Mathematics, A Wiley-Interscience Publication.

[Dem97] Peter Dembowski. *Finite geometries*. Classics in Mathematics. Springer-Verlag, Berlin, 1997. Reprint of the 1968 original.

[Dic58] Leonard Eugene Dickson. *Linear groups: With an exposition of the Galois field theory*. with an introduction by W. Magnus. Dover Publications Inc., New York, 1958.

[KLS08] Chandrashekhar Khare, Michael Larsen, and Gordan Savin. Functoriality and the inverse Galois problem. *Compos. Math.*, 144(3):541–564, 2008.

[LZ82] Shang Zhi Li and Jian Guo Zha. On certain classes of maximal subgroups in $\mathrm{PSp}(2n,\ F)$. *Sci. Sinica Ser. A*, 25(12):1250–1257, 1982.

[Mit11] Howard H. Mitchell. Determination of the ordinary and modular ternary linear groups. *Trans. Amer. Math. Soc.*, 12(2):207–242, 1911.

[Mit14] Howard H. Mitchell. The subgroups of the quaternary abelian linear group. *Trans. Amer. Math. Soc.*, 15(4):379–396, 1914.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser77] Jean-Pierre Serre. *Linear representations of finite groups*. Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[Wag74] Ascher Wagner. Groups generated by elations. *Abh. Math. Sem. Univ. Hamburg*, 41:190–205, 1974.